On the Rudin-Shapiro transform

la Cour-Harbo, Anders

Published in:
Applied and Computational Harmonic Analysis

DOI (link to publication from Publisher):
10.1016/j.acha.2007.05.003

Publication date:
2008

Document Version
Accepted author manuscript, peer reviewed version

On the Rudin-Shapiro Transform

A. la Cour-Harbo [1]

Aalborg University, Department of Control Engineering, Fredrik Bajers Vej 7C, 9220 Aalborg East, Denmark.

Abstract

The Rudin-Shapiro transform (RST) is a linear transform derived from the remarkable Rudin-Shapiro polynomials discovered in 1951. The transform has the notable property of forming a spread spectrum basis for $\mathbb{R}^N$, i.e. the basis vectors are sequences with a nearly flat power spectrum. It is also orthogonal and Hadamard, and it can be made symmetric. This presentation is partly a tutorial on the RST, partly some new results on the symmetric RST that makes the transform interesting from an applicational point-of-view. In particular, it is shown how to make a very simple $O(N \log N)$ implementation, which is quite similar to the Haar wavelet packet transform.

Key words: Rudin-Shapiro polynomials, spread spectrum, Haar transform
PACS:

The Rudin-Shapiro transform was originally conceived as a series of coefficient sequences from a set of trigonometric polynomials discovered by Shapiro and Rudin in the 1950's. Since then the transform has come to exist in its own right. This is because the transform has a series of nice properties among which the spread spectrum property of the basis elements is the most noticeable one. The transform proves useful for designing signals in low-cost hardware, not least due to the existence of a fast and numerically robust implementation.

The Rudin-Shapiro polynomials are categorized as flat polynomials. This refers to the fact that the amplitude of the complex polynomials are, on the unit circle, bounded by a constant times the energy of the polynomial. There exists many other examples of flat polynomials besides the Rudin-Shapiro polynomials, and the history of the development in the field of flat polynomials is quite interesting. This is in no small part due to the fact that a number of seemingly simple questions within the field have remained unanswered for several decades.

[1] This work is supported by the Danish Technical Science Foundation (STVF) Grant no. 9701481

Flat polynomials are also interesting for applications. The author has demonstrated, see la Cour-Harbo [23] that a spread spectrum transform has a role to play in the attempt to increase the robustness of active sensors. In that context the aim of this presentation is to show the mathematical background for properties exploited in real applications.

The paper is divided into four parts (sections). Section 1 reviews some of the important definitions and notions in the field of flat polynomials. This is followed by a short historical background listing some of the major contributions in this field. In Section 2 the classical Rudin-Shapiro polynomials are presented along with some previously known results on the crest factor and auto and cross correlation properties of RS polynomials.

A matrix formulation of the recursive construction of the RS polynomials leading to a transform matrix is presented in Section 3. As the title suggests the author has denoted this transform *Rudin-Shapiro Transform* for obvious reasons. The RST has also been named PONS (Prometheus Orthonormal Set) by Byrnes, see for instance [9].

Section 4 holds the main result. Here a matrix formulation of the recursive construction of the symmetric RST is given in Definition 9, followed by Theorem 10, which shows that this construction yields a symmetric transform with all the desired properties inherited from the non-symmetric transform. The definition of the symmetric RST also contains a factorization of the transform matrix, which enables an $O(N \log N)$ implementation of the matrix multiplication. This is presented and discussed in Section 4.2 and 4.3.

Finally, three conjectures on RS polynomials that the author has been unable to prove are stated in Section 4.4.

1 SEARCH FOR FLAT POLYNOMIALS

The construction of flat polynomials dates back to the beginning of 20th century. Of course, at that time the purpose was not to design signals for use in digital transmission systems. The incitement then was rather a mathematical interest in certain 'nice' trigonometric series. One of the early examples of flat polynomials is a discovery by in 1916 by Hardy and Littlewood [19]. They investigated the series

$$\sum_{n=1}^{\infty} e^{ikn\log n} \frac{e^{in\xi}}{n^{1/2+\alpha}}, \quad k, \alpha \neq 0. \tag{1}$$

as part of a study of so-called elliptic Theta-functions. When $\alpha = -1/2$ the partial sum $|s_N(\xi)|$ is uniformly bounded by $C\sqrt{N}$ on $[0; 2\pi]$ with C depending only on k (Zygmund [40]). This makes the polynomial flat in some sense because there

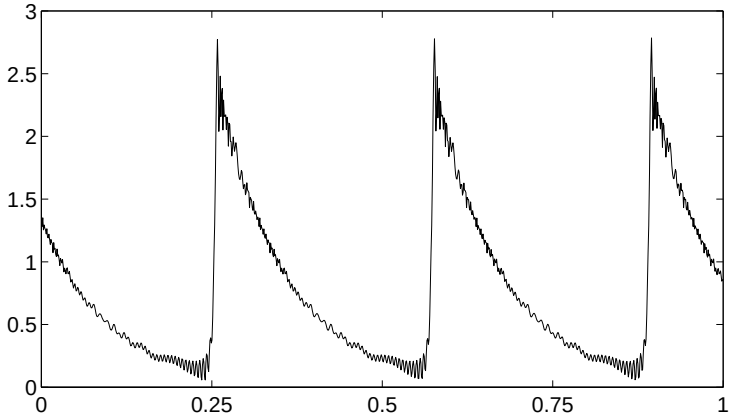

Fig. 1. The polynomial (1) with $\alpha = -1/2$ and $k = 1$, here shown with the first 1000 terms of the sum. The coefficient set is normalized to have ℓ_2 norm 1.

is a limit to how concentrated the energy can be in the Fourier domain. No explicit bound is given by Zygmund, but a few numerical experiments reveals that $C > 3\sqrt{2\pi}$ for $k = 1$. This is somewhat high compared to limits for other series discovered since then. The polynomial is shown in Fig. 1, which incidentally it below 3. This is due to the resolution of the calculations and the graph. Zooming in on the third top reveals that it, with sufficiently many terms of the sum, does reach above 3.

The interest in flat polynomials still exists today, though the interest is now in general fuelled by the need for pseudo random sequences suitable for application in fields such as transmission and encryption. Therefore it is research in information theory rather than pure mathematics that produces new results in the field of flat polynomials, and many interesting results have indeed emerged. This is not to say that recent mathematical results do not exist. For instance, in the field of wavelets, a construction of Coifman et al. [13] called Noiselets is based on the idea of generating sequences, which are uncompressible by a Haar-Walsh wavelet packet transform, i.e. the transform coefficients exhibits no decay. The result is sequences of ± 1 and $\pm i$ that have the same type of flatness as Rudin-Shapiro sequences (see later).

This presentation of the RST is also of mathematical nature. For applications of the RST, see for instance Byrnes et al. [11,10], Byrnes [9], Tseng [39], Nazarahty et al. [28], la Cour-Harbo [23].

1.1 Notation

Before venturing into a search for flat polynomials it is convenient to fix the notation. First unimodular sequences are defined. They will become the coefficients in the flat polynomials.

Definition 1 (Unimodular sequences) *Define the sets of unimodular sequences as*

$$\mathscr{S}_N^p = \left\{ \beta \in \mathbb{C}^N \;\middle|\; \beta_k \in \{e^{i2\pi m/p}\}_{m=0,\ldots,p-1} \right\}, \quad p = 2, 3, \ldots ,$$

which means the set of N dimensional vectors with entries in a set of equidistantly sampled points on the unit circle in $\mathbb{C}$. Define also the natural extension

$$\mathscr{S}_N^\infty = \left\{ \beta \in \mathbb{C}^N \;\middle|\; \beta_k \in \{e^{i2\pi\alpha_k}\}_{\alpha_k \in [0;1)} \right\}$$

for $p = \infty$.

The polynomials are defined on the unit circle in the complex plane, and takes coefficients from the set of unimodular sequences. Note how the defined polynomials are the Fourier transform of the unimodular sequences, and thus that the ℓ^2 norm of such a sequence equals the length of the sequence.

Definition 2 (Trigonometric Polynomials) *Define the sets of complex trigonometric polynomials*

$$\mathscr{H}_N^p = \left\{ f_N : \mathbb{R} \mapsto \mathbb{C} \;\middle|\; f_N(\xi) = \sum_{k=0}^{N-1} \beta_k e^{i2\pi k\xi} \right\}, \quad \beta \in \mathscr{S}_N^p, \quad \xi \in [0;1)$$

for $p = 2, 3, \ldots, \infty$. Define also

$$\mathscr{H}^p = \bigcup_{n=1}^{\infty} \mathscr{H}_n^p.$$

Note that in most literature, see for instance Littlewood [26], only the two sets $\mathscr{H}^2$ and $\mathscr{H}^\infty$ are mentioned, and they are typically referred to as $\mathscr{F}$ and $\mathscr{G}$.

It is also interesting to note that the set $\mathscr{H}^2$ differs from the rest in being the only one with exclusively real coefficients (± 1's). This makes it by far the most interesting set from an applicational point of view. The Rudin-Shapiro polynomials are examples of $\mathscr{H}^2$ functions.

Finally, one should note that it is only a matter of taste whether the lower and upper bound on the sum should be 0 and $N-1$, respectively, 0 and N, or 1 and N. There seems to be no preference in the existing literature, and here the bounds are chosen to correspond with the general notion that, as default, the first index in a vector is 0, and that the dimension of the sequence spaces (to which β belongs) should correspond to the 'dimension' of the function spaces $\mathscr{H}^p$.

It is surprising that the set $\mathscr{H}^p$, which is simply a collection of Fourier transformed sequences taken from the unit circle, has been subject to extensive investigations throughout the past 50 years, and that some seemingly simple questions are rather difficult to answer. The Fourier transform is arguable the best understood and most popular tool in harmonic analysis, and thus one is inclined to believe that a set such as $\mathscr{H}^p$ would be well-described by now.

The search for flat polynomials is basically a search for an answer to the question: How close can a function $f_N \in \mathscr{H}^p$ come to satisfying $|f_N| = \sqrt{N}$ for arbitrarily large N? The question is quite intriguing because on the one hand the equality is never reached for finite N. This can be seen in the following way. Let $f_N \in \mathscr{H}^p_N$, $p \geq 2$. Since $\|f_N\|_2 = \|\mathbf{c}\|_2 = \sqrt{N}$, $\mathbf{c}$ being the Fourier coefficients of f_N, and since $\|f_N\|_2 \leq \|f_N\|_\infty$ on the unit interval, we have that $\|f_N\|_\infty \geq \sqrt{N}$. Assuming now that $|f_N(\xi)| = \sqrt{N}$ then, for $|\beta_k| = 1$,

$$N = |f_N(\xi)|^2 = \left|\sum_{m=0}^{N-1} \beta_m e^{i2\pi m\xi}\right|^2 = \sum_{m=-N+1}^{N-1} (\beta * \overline{\beta})_m e^{im\xi}$$
$$\Rightarrow \quad (\beta * \overline{\beta})_m = \delta[m] \quad \Rightarrow \quad \beta_0\beta_{N-1} = 0,$$

which is a contradiction. On the other hand, the Rudin-Shapiro polynomials introduced in Section 2 demonstrate that for $\mathscr{H}^2$ (and indeed for $\mathscr{H}^{2p}$ and $\mathscr{H}^\infty$) there is a uniform upper bound for the deviation of $|f_N|$ from $\sqrt{N}$. From (7) it is seen that this bound is $\sqrt{2}$, since $|P_n(\xi)| \leq \sqrt{2}\sqrt{2^n}$.

The question of how close a function $f_N \in \mathscr{H}^p$ can come to $\sqrt{N}$ might also involve a lower bound. Moreover, there may even exist polynomials such that $f_N(\xi)/\sqrt{N} \to 1$ uniformly in ξ for $N \to \infty$. The latter would certainly qualify as a flat polynomial. In the course of this presentation it becomes necessary to distinguish between four different types of flatness.

Definition 3 (Flat Polynomials) *Define for a function $f_N \in \mathscr{H}^p$ the following terms associated with the given inequalities.*

Flatness	*Condition*
Semi-flat	$\|f_N\| \leq B\sqrt{N}$
Near-flat	$0 < \|f_N\| < B\sqrt{N}$
Flat	$A\sqrt{N} \leq \|f_N\| \leq B\sqrt{N}$
Ultra-flat	$(1 - \|o(1)\|)\sqrt{N} \leq \|f_N\| \leq (1 + \|o(1)\|)\sqrt{N}$

The constants A and B are independent of N and satisfy $0 < A \leq B$.

In many scenarios, particularly in real applications, this distinction is less important

as even the semi-flat polynomials exhibits spread spectrum properties (at least for reasonably small B). The discussion of the properties of the trigonometric polynomials in $\mathscr{H}^p$ in respect to different types of flatness is thus of a more academical nature.

While the type of flatness is often of minor interest in real applications it is often interesting to know the ratio between the sup norm and the L^2 norm. This is know as the crest factor, and can be computed for any sequences $\mathbf{c} \in \mathbb{C}^N$. As shown above this factor is always > 1 for finite sequences. To fix notation the following definition is provided.

Definition 4 (The Crest Factor) *For any sequence $\mathbf{c} \in \mathbb{C}^N$ define the polynomial*

$$P(\xi) = \sum_{n=0}^{N-1} c_n e^{i2\pi n\xi}, \quad \xi \in [0; 1).$$

The crest factor C for any sequence $\mathbf{c} \in \mathbb{C}^N$ is defined as

$$C(\mathbf{c}) \equiv \frac{\|P\|_\infty}{\|P\|_2} = \frac{\|P\|_\infty}{\|\mathbf{c}\|_2},$$

where the later equality follows from Parseval's equation.

Since the crest factor quantifies the amplitude of the Fourier transform of $\mathbf{c}$ it is an indicator for the 'frequency flatness' or 'frequency spreading' of the sequence $\mathbf{c}$. In some literature the crest factor is known as peak-to-mean ratio or peak-to-mean power envelope ratio.

Before turning to the Rudin-Shapiro transform, the author would like to give a very short historical presentation of the quest for flat polynomials.

1.3 Historical Background

Many people have contributed to the development of flat polynomials, and many papers have been written on the subject. Some publications are hard to come by, either because their date back many decades, or because they are local journals of universities, academies, and the like. Consequently, this presentation is not exhaustive and serves only as background information for interested readers. A summary is found in Table 1. Thanks are due to the library at Department of Mathematics at KTH, Stockholm, for assistance in locating some of the papers referred below.

The first clue to Rudin-Shapiro polynomials came in 1949 when Golay published a paper entitled 'Multislit spectrometry' [16] introducing the notion of pairs of complementary sequences. Although the definition from then does not immediately reveal it, complementary sequences are coefficients in flat polynomials. The theory

		There exist polynomials of type			
		Semiflat		Flat	Ultraflat
$\mathscr{H}^\infty$ in the set	$\subset [0;1)$		Crest factor		Littlewood, 1966 [26] Byrnes, 1977 [7]
	$= [0;1)$	Hardy, Littlewood, 1916 [19] Littlewood, 1966 [26] Beller, 1971 [3]	> 3 1.36 1.1717	Clunie 1959 [1] [12] Körner, 1980 [22]	Cj. $\emptyset$ [2] Erdös, 1957 [14] Kahane, 1980 [21]
$\mathscr{H}^p$	$\subset [0;1)$			Beck, 1990 ($p = 3$) [3] [2]	Beck, 1990 ($p = 3$) [4] [2]
	$= [0;1)$	Coifman et. al., 1994 ($p = 4$) [5] [13]	$\sqrt{2}$	Beck, 1990 ($p = 400$) [2]	$\emptyset$: Fredman et al. 1989 [6] [15]
$\mathscr{H}^2$	$\subset [0;1)$	Cj. nearflat, la Cour-Harbo, 2000	$\sqrt{2}$		
	$= [0;1)$	Shapiro, Rudin, 1951/59 [7] [33] Shapiro, Rudin, 1951/59 [8] [33] Brillhart, Morton, 1978 [8] [6] France, Tenenbaum, 1981 [8] [27] Saffari, 1986 [8] [34] Allouche, France, 1985 [9] [1]	$\sqrt{2}$ $2 + 2\sqrt{2}$ $\geq \sqrt{6}$ $2 + \sqrt{2}$ $(2 + \sqrt{2})\sqrt{\frac{3}{5}}$ $2 + \sqrt{2}$		Cj. $\emptyset$ Erdös, 1957 [14] Cj. $\emptyset$ Saffari, Smith, 1990 [35]

[1] Coefficients in the unit disc.
[2] Conjectured empty.
[3] For half the unit circle.
[4] For sufficiently small neighborhood of 0.
[5] For signal length 2^j
[6] In L^4 norm and for coefficients satisfying $\beta = \overline{\beta}$
[7] Rudin-Shapiro sequences.
[8] All partial Rudin-Shapiro sequences.
[9] All 2-multiplicative sequences.

Table 1. Review of some of the results obtained in the search for flat polynomials.

was further develop in 1951 [17] and 1962 [18]. Since then others have further refined the theory to include whole classes of complementary sequences and to include multiphase series instead of just ± 1's.

In the mean time, the same idea was discovered by mathematicians and formed a independent line of investigation. Harold Shapiro had studied extremal problems of trigonometric series in his Master's thesis from 1951 [36], and from this derived examples of complementary sequences (although he does not refer to them by this name). On page 39 in the thesis the definition of Rudin-Shapiro polynomials is given, and the crest factors $\sqrt{2}$ for length 2^n and $2 + 2\sqrt{2}$ for arbitrary length are deduced. These results were rediscovered in 1959 by Rudin [33] who, with the accept of Shapiro published the paper 'Some theorems on Fourier coefficients' which introduced the construction as it is shown in the next section.

In 1957 Paul Erdös presented at a symposium at Assumption University of Windsor a list of 28 so far unsolved problems [14]. Number 22 reads: If $f_N \in \mathscr{H}^\infty$, does there exist a universal constant $c > 0$ such that $\|f_N\|_\infty > (1 + c)\sqrt{N}$? This is the opposite of conjecturing than there exists ultra-flat polynomials $f_N \in \mathscr{H}^\infty$. The existence of such polynomials was confirmed in 1980 by Kahane [21]. And in 1989 Fredman et al. [15] proved that $\|f_N\|_4 > 1.1048^{1/4}\sqrt{N}$ when $\beta = \bar{\beta}$. Erdös claimed that he had an unpublished proof that

$$\Big\| \sum_{k=0}^{N} \beta_k \cos k\theta \Big\|_\infty > (1 + c)\sqrt{N/2}\,,$$

which is a variation on the theme. He did not reveal the value of the constant c, though. He also mentioned, as problem number 26, one of the hardest questions to settle, that is, the question of whether there exists a flat $f_N \in \mathscr{H}^2$.

While the engineers who took an interest in flat polynomials were looking for binary sequences with nice autocorrelation properties, the interest on the mathematicians' part was in peak values of polynomials defined with a set of restrictions. These typically included unimodular coefficients (as defined above) and restriction to the unit circle in $\mathbb{C}$. Many other restrictions have been applied, probably due to the difficulty in achieving any significant results.

In 1965 Newman [29] investigated the problem of creating a truly flat polynomial in L^1 norm. He presents a certain construction which yields flat polynomials in L^1 as well as in L^4. The same challenge was also taken up by Littlewood in 1962 [25], though he attempted the construction in L^2 norm. He showed that the function

$$\sum_{m=0}^{N-1} \exp\Big(\frac{1}{2} m(m+1)\theta\pi i/N\Big)$$

tends to 1 uniformly for $N \to \infty$ on $N^{-1/2+\delta} \leq |\theta| \leq \pi$ (but fails outside this interval). Littlewood states explicitly that he has made extensive, although futile

attempts to modify the construction to achieve uniform convergence for all θ.

In 1980 Körner [22], using a construction by Byrnes [7], proved that there exists flat polynomials $f_N \in \mathscr{H}^\infty$. Soon after Kahane [21] significantly improved this by disproving problem number 22 by Erdös and thus showing the existence of ultra-flat polynomials. This is one of the major results in the field of flat polynomials.

The existence of ultra-flat polynomials with real, unimodular coefficients have been very difficult to settle. A number of mathematicians have actually published works proving as well as disproving the existence. The author has not been able to determine whether the question has indeed been settled definitively.

2 CLASSICAL RUDIN-SHAPIRO POLYNOMIALS

The first discovery of systematic construction of sequences that are somewhat flat in the frequency domain was made by Golay in 1949 [16], as was stated in the previous section. He introduced the notion of complementary sequences. A pair of binary complementary sequences is defined as a pair of equally long, finite sequences of $+1$'s and -1's such that the sum of the aperiodic autocorrelation coefficients of the two sequences is zero for all but the zero shift. Later he further developed the theory of such pairs, see Golay [18], showing that one set of sequences could produce several others.

The idea of complementary sequences was discovered independently by Shapiro in his 1951 Master's thesis [36]. According to Shapiro, he 'accidentally' made the discovery as he was working on extremal problems for polynomials. He thus had a mathematical approach to the subject whereas Golay took a more engineering approach. The Shapiro result was rediscovered by Rudin and published in 1959 [33], and is now known as the Rudin-Shapiro polynomials. The construction is recursive and generates a pair of semi-flat polynomials, though with difference crest factor for polynomial order equal to and different from a power of 2. Actually, the coefficients in these polynomials are the very same as the binary Golay complementary sequences. This is easily verified once the Rudin-Shapiro polynomials have been defined, see Section 2.2.

2.1 Rudin-Shapiro Polynomials

The Rudin-Shapiro polynomials are defined recursively as

$$P_{n+1}(\xi) = P_n(\xi) + e^{i2\pi 2^n \xi} Q_n(\xi), \quad P_0 = 1\ , \tag{2}$$

$$Q_{n+1}(\xi) = P_n(\xi) - e^{i2\pi 2^n \xi} Q_n(\xi), \quad Q_0 = 1\ , \tag{3}$$

for $\xi \in [0;1)$. The coefficients of the first few polynomials are

$$\begin{aligned}
P_0 &: 1 \\
Q_0 &: 1 \\
P_1 &: 1 \quad 1 \\
Q_1 &: 1 \; -1 \\
P_2 &: 1 \quad 1 \quad 1 \; -1 \\
Q_2 &: 1 \quad 1 \; -1 \quad 1 \\
P_3 &: 1 \quad 1 \quad 1 \; -1 \quad 1 \quad 1 \; -1 \quad 1 \\
Q_3 &: 1 \quad 1 \quad 1 \; -1 \; -1 \; -1 \quad 1 \; -1
\end{aligned} \tag{4}$$

It is obvious that the sequences are generated by a simple 'append rule'. We will refer to the coefficients of the RS polynomials as RS sequences. The ingenuity of these polynomials is the combination of fixed sized coefficients and the alternating sign in the recursive construction of P and Q. The former property gives

$$\|P_n\|_2^2 = \sum_{k=0}^{2^n-1} (\pm 1)^2 = 2^n, \tag{5}$$

while the latter property gives

$$|P_n(\xi)|^2 + |Q_n(\xi)|^2 = 2|P_{n-1}(\xi)|^2 + 2|Q_{n-1}(\xi)|^2 = 2^{n+1}, \tag{6}$$

since $|e^{i2\pi 2^n \xi}| = 1$. This leads to

$$|P_n(\xi)| \leq \sqrt{2} \cdot 2^{n/2}, \quad \forall \xi \in [0;1) \; ,$$

that is, a uniform upper bound for P_n. Now, combining (5) and (6) yields the squared crest factor

$$\frac{\|P_n\|_\infty^2}{\|P_n\|_2^2} \leq 2 \; . \tag{7}$$

This means that $|P_n(\xi)|^2$, $\xi \in [0;1)$, is a function that lies within the rectangle $[0;1] \times [0;2^{n+1}]$, and at the same time 'covers' exactly half of its area. This guarantees the polynomial to be somewhat flat. Two examples of $|P_n|$ are shown in Fig. 2. At this point it is important to realize that the term 'flat' should be understood as 'not excessively far from a constant function', but not necessarily 'close to a constant function'. This was also hinted in Definition 3. To demonstrate the importance of this concept the two lower most graphs in Fig. 2 show that neither the well-known (an often used in applications) square wave nor a random ± 1 sequence can be considered flat.

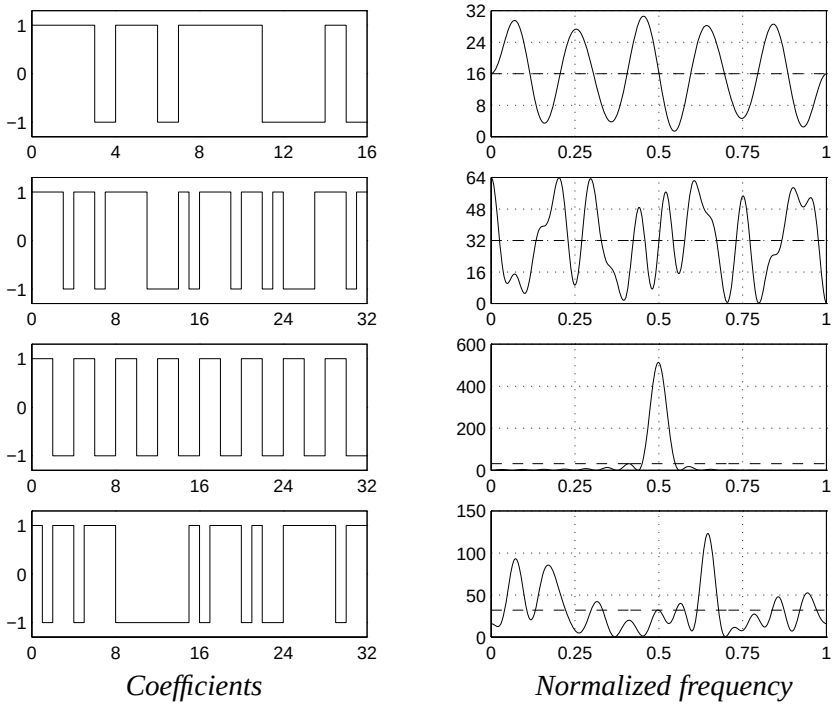

Fig. 2. The coefficients (left) and squared amplitude (right) of the Rudin-Shapiro polynomials P_4 and P_5. Below the coefficients and squared amplitude of the Fourier transform of a square wave and a random sequence. The horizontal dashed lines are the energy of the signals.

2.2 Properties of Rudin-Shapiro Polynomials

The construction of the RS polynomial is such that the parallelogram law

$$|a+b|^2 + |a-b|^2 = 2|a|^2 + 2|b|^2$$

is the only means needed for achieving the $\sqrt{2}$ crest factor. This property is in fact essential for the relation between RS sequence and Golay complementary sequences. In terms of RS polynomials the law gives (6), i.e. that

$$P_n(\xi)\overline{P_n(\xi)} + Q_n(\xi)\overline{Q_n(\xi)} = 2^{n+1} \ .$$

Applying the inverse Fourier transform yields

$$(\mathbf{p} * \overline{\mathbf{p}})[k] + (\mathbf{q} * \overline{\mathbf{q}})[k] = 2^{n+1}\delta[k] \ , \tag{8}$$

for $-2^n + 1 \leq k \leq 2^n - 1$, where $\mathbf{p}$ and $\mathbf{q}$ are the coefficients sequences of P and Q, respectively, and $\overline{\mathbf{p}}$ means the time reversed of $\mathbf{p}$. Notice that (8) is exactly the definition of a set of complementary sequences.

While the crest factor of $\sqrt{2}$ was easily derived the computations leading to that result did not show whether in fact a smaller upper bound is possible. The follow-

ing lemma demonstrates that for at least some RS polynomials the crest factor is correct, i.e. the upper bound on the peak-to-mean ratio cannot be smaller.

Lemma 5 *Let P and Q be defined by* (2) *and* (3)*. Then*

$$\begin{aligned} P_{2m}(0) &= 2^m, \quad P_{2m}(1/2) = 2^m, \qquad P_{2m+1}(0) = 2^{m+1}, \quad P_{2m+1}(1/2) = 0 \\ Q_{2m}(0) &= 2^m, \quad Q_{2m}(1/2) = -2^m, \quad Q_{2m+1}(0) = 0, \qquad Q_{2m+1}(1/2) = 2^{m+1}. \end{aligned}$$

Proof First note that

$$\begin{aligned} P_{n+2}(\xi) &= P_{n+1}(\xi) + e^{i2\pi 2^{n+1}\xi} Q_{n+1}(\xi) \\ &= P_n(\xi) + e^{i2\pi 2^n \xi} Q_n(\xi) + e^{i2\pi 2^{n+1}\xi}\Big(P_n(\xi) - e^{i2\pi 2^n \xi} Q_n(\xi)\Big) \\ &= (1 + e^{i2\pi 2^{n+1}\xi}) P_n(\xi) + e^{i2\pi 2^n \xi}(1 - e^{i2^{n+1}\xi}) Q_n(\xi). \end{aligned} \tag{9}$$

Then for $n = 2m - 2$ we have

$$\begin{aligned} P_{2m}(0) &= (1+1)P_{2m-2}(0) + 0 = \cdots = 2^m P_0(0) = 2^m, \\ P_{2m}(1/2) &= 2P_{2m-2}(1/2) = 2^m P_0(1/2) = 2^m, \end{aligned}$$

and for $n = 2m - 1$

$$\begin{aligned} P_{2m+1}(0) &= 2P_{2m-1}(0) = 2^m P_1(0) = 2^{m+1}, \\ P_{2m+1}(1/2) &= 2P_{2m-1}(1/2) = 2^m P_1(1/2) = 0. \end{aligned}$$

Equivalent calculations yield the results for the Q polynomials. □

The idea to these calculation is from Brillhart [5]. Also, the P and Q polynomials are anti-symmetric around $1/4$, as this lemma demonstrates.

Lemma 6 *Let $\mathbf{p}, \mathbf{q}$ be two Rudin-Shapiro sequences. Then*

$$\begin{aligned} |P_n(\xi)|^2 &= 2^{n+1} - |P_n(1/2 - \xi)|^2 \\ |Q_n(\xi)|^2 &= 2^{n+1} - |Q_n(1/2 - \xi)|^2. \end{aligned}$$

Proof The lemma obviously holds for $n = 0$. Then the result follows from an induction argument.

$$\begin{aligned} |P_{n+1}(\xi)|^2 &= |P_n(\xi)|^2 + |Q_n(\xi)|^2 + e^{i2\pi 2^n \xi}\overline{P_n(\xi)} Q_n(\xi) + e^{-i2\pi 2^n \xi} P_n(\xi)\overline{Q_n(\xi)} \\ &= 2^{n+1} - |P_n(1/2 - \xi)|^2 + 2^{n+1} - |Q_n(1/2 - \xi)|^2 \\ &\quad + 2\,\mathrm{Re}\Big\{e^{i2\pi 2^n \xi}\overline{P_n(\xi)} Q_n(\xi)\Big\} \\ &= 2^{n+2} - |P_n(1/2 - \xi)|^2 - |Q_n(1/2 - \xi)|^2 \\ &\quad - 2\,\mathrm{Re}\Big\{e^{i2\pi 2^n (1/2 - \xi)}\overline{P_n(1/2 - \xi)} Q_n(1/2 - \xi)\Big\} \\ &= 2^{n+2} - |P_{n+1}(1/2 - \xi)|^2. \end{aligned}$$

Since P and Q are trigonometric polynomials the third equality is given by a calculation that involves the equality $\cos(\xi) = -\cos(\pi - \xi)$. □

The following lemma shows that the append rule presented for the Rudin-Shapiro sequences, i.e. the rule used to produce longer sequences, actually results in a rather nice property. Namely that the cross correlation of $\mathbf{p}$ and $\mathbf{q}$ is zero for even shifts, and the autocorrelation is zero for even shifts except the zero shift.

Lemma 7 *Let $\mathbf{p}, \mathbf{q} \in \mathbb{C}^N$ be two vectors with the properties*

$$\langle \tau_{2k}\mathbf{p}, \mathbf{q} \rangle = 0, \qquad \langle \tau_{2k}\mathbf{p}, \mathbf{p} \rangle = \langle \tau_{2k}\mathbf{q}, \mathbf{q} \rangle = C\delta[k],$$

where τ_m means a shift of index by $+m$. Define

$$\tilde{\mathbf{p}} = \begin{bmatrix} \mathbf{p} \\ \mathbf{q} \end{bmatrix} \quad \textit{and} \quad \tilde{\mathbf{q}} = \begin{bmatrix} \mathbf{p} \\ -\mathbf{q} \end{bmatrix}.$$

Then

$$\langle \tau_{2k}\tilde{\mathbf{p}}, \tilde{\mathbf{q}} \rangle = 0, \qquad \langle \tau_{2k}\tilde{\mathbf{p}}, \tilde{\mathbf{p}} \rangle = \langle \tau_{2k}\tilde{\mathbf{q}}, \tilde{\mathbf{q}} \rangle = 2C\delta[k].$$

Note that $\langle \tau_{2k}\mathbf{p}, \mathbf{q} \rangle = (\mathbf{p} * \bar{\mathbf{p}})[-2k]$.

Proof From the definitions of $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ it follows that

$$\left.\begin{matrix} \langle \tau_{2k}\tilde{\mathbf{p}}, \tilde{\mathbf{q}} \rangle \\ \langle \tau_{2k}\tilde{\mathbf{p}}, \tilde{\mathbf{p}} \rangle \\ \langle \tau_{2k}\tilde{\mathbf{q}}, \tilde{\mathbf{q}} \rangle \end{matrix}\right\} = \begin{cases} \pm \langle \tau_{2k+N}\mathbf{p}, \mathbf{q} \rangle & \text{for } k = -N+1, \ldots, -N/2, \\ \langle \tau_{2k}\mathbf{p}, \mathbf{p} \rangle \pm \langle \tau_{2k}\mathbf{q}, \mathbf{q} \rangle \pm \langle \tau_{2k+N}\mathbf{p}, \mathbf{q} \rangle & \text{for } k = -N/2+1, \ldots, -1, \\ \langle \tau_{2k}\mathbf{p}, \mathbf{p} \rangle \pm \langle \tau_{2k}\mathbf{q}, \mathbf{q} \rangle \pm \langle \tau_{2k-N}\mathbf{p}, \mathbf{q} \rangle & \text{for } k = 1, \ldots, N/2-1, \\ \pm \langle \tau_{2k-N}\mathbf{p}, \mathbf{q} \rangle & \text{for } k = N/2, \ldots, N-1. \end{cases}$$

All four expressions equal zero independently of the signs. For the zero shift

$$\langle \tilde{\mathbf{p}}, \tilde{\mathbf{q}} \rangle = \langle \mathbf{p}, \mathbf{p} \rangle - \langle \mathbf{q}, \mathbf{q} \rangle = 0 \,,$$

and

$$\langle \tilde{\mathbf{p}}, \tilde{\mathbf{p}} \rangle = \langle \tilde{\mathbf{q}}, \tilde{\mathbf{q}} \rangle = \langle \mathbf{p}, \mathbf{p} \rangle + \langle \mathbf{q}, \mathbf{q} \rangle = 2C \,.$$

□

An obvious consequence of this lemma is

Corollary 7.1 *Any Rudin-Shapiro sequence set $\mathbf{p}, \mathbf{q}$ have the property $\langle \tau_{2k}\mathbf{p}, \mathbf{q} \rangle = 0$.*

A more general statement about the autocorrelation of RS sequences is given in Taghavi [38] and [37]. The results are presented in the following lemma.

Lemma 8 *Let* $\mathbf{p}$ *be a RS sequence of length* 2^N*. Then*

$$\left|\langle \tau_k \mathbf{p}, \mathbf{p} \rangle\right| \leq 3.2134 \cdot 2^{0.7303N}$$

for $k = -N+1, \ldots, N-1$*. Further there exists* C *such that*

$$\left|\langle \tau_k \mathbf{p}, \mathbf{p} \rangle\right| > C 2^{0.73N} \ .$$

In applications it is often very useful to have spread spectrum sequences with a good autocorrelation, i.e. where only the zero lag is significantly different from zero. Such sequences have been systematically constructed by No et al., see [30–32].

3 THE RUDIN-SHAPIRO TRANSFORM

An interesting property of the RS sequences generated according to the appending rule in (2) and (3) is that they are orthogonal. This is immediately evident from the appending example shown. It is also worth noting that interchanging the $+$ and $-$ in (2) and (3) would still produce sequences with all the previously presented properties. In fact, arbitrarily interchanging the signs in each recursive step does not affect the properties of the constructed sequences.

An elegant construction achieving all combinations of sign changes is found in Benke [4] (Byrnes [8,10] gives a similar construction). In short,

$$\begin{bmatrix} P_{n+1,\epsilon}(\xi) \\ Q_{n+1,\epsilon}(\xi) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\epsilon_n} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi 2^n \xi} \end{bmatrix} \begin{bmatrix} P_{n,\epsilon}(\xi) \\ Q_{n,\epsilon}(\xi) \end{bmatrix}, \tag{10}$$

where $\epsilon_n \in \{0, 1\}$ is chosen in each step. A total of 2^n different P polynomials are possible after n steps. Thus, two P polynomials with each two coefficients are obtained after one steps, four P polynomials with each four coefficients are obtained after two steps, and so on. The two and four polynomials have coefficients (here inserted as rows)

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix},$$

and the eight P polynomials after the third step have coefficients

$$\begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 \end{bmatrix}.$$

Note that all rows in the matrices are orthogonal. Thus, the RS sequences of length 2^J constitutes an orthogonal basis of $\mathbb{R}^{2^J}$. Consequently, the matrices are called the Rudin-Shapiro transform (RST). It is shown in Benke [4] that this construction can be generalized in various ways.

The individual entries in the Rudin-Shapiro transform can be found by the following equation, where $\mathbf{P}^{(N)} \equiv \left[p_{m,n}^{(N)}\right]$ is the $2^N \times 2^N$ RST matrix.

$$p_{m,n}^{(N)} = \prod_{k=1}^{N} (-1)^{n_k(m_{N-k+1}+n_{k-1})}, \quad n_0 \equiv 0.$$

The n_k and m_k is the k'th binary digit of n and m respectively, with $k = 1$ as LSB. This property is not proved at this points as a very similar equation is given and proved in the next section.

Applying the RST decomposes a signal into a basis of elements with a spread spectrum property. This is in some sense the opposite of a Fourier transform which is a decomposition into a narrow spectrum basis. The transform is orthogonal (up to a scaling) and thus energy preserving, and the equal amplitude of all the entries makes the transform numerical stable. In general, it is an appealing transform for design and analysis of spread spectrum signals. However, at this point a fast implementation is still missing. Matrix multiplication is a $O(N^2)$ operation, and in general it is preferable, if not desirable, to have an $O(N \log N)$ implementation, especially for real time applications.

Note also that while the rows of the presented matrices do have a low crest factor, this is not the case for the columns which exhibits a Walsh-like structure rather than spread spectrum structure.

The problems mentioned here are addressed in the next section, where a slight change of the recursive definition of the RS polynomials yields a symmetric RS

transform. At the same time a fast implementation, actually $O(N \log N)$ with a small constant, is also given.

4 THE SYMMETRIC RUDIN-SHAPIRO TRANSFORM

This section holds the main result in of this presentation; the recursive matrix construction and factorization of the symmetric RST, and the subsequent fast implementation of the transform matrix. It is also proven that this matrix construction inherits all the nice properties of the non-symmetric construction.

The construction starts with the observation that the Rudin-Shapiro transform can indeed be made symmetric. The idea for this is communicated in Byrnes et al. [10]. There the polynomials are defined by a modification of the previously presented definition in (2) and (3). The following equations have been slightly rewritten compared to [10], to comply with the notation in this presentation (most significantly, Byrnes have discarded the Q polynomials in favor of a more advanced indexing of the P polynomials). The symmetric RST is derived from the following equations.

$$\begin{aligned}
P_{j+1,4m}(\xi) &= P_{j,2m}(\xi) \phantom{+P_{j,2m+1}(\xi)} + e^{i2\pi 2^j\xi}Q_{j,2m+1}(\xi),\\
P_{j+1,4m+1}(\xi) &= P_{j,2m}(\xi) \phantom{+P_{j,2m+1}(\xi)} - e^{i2\pi 2^j\xi}Q_{j,2m}(\xi),\\
P_{j+1,4m+2}(\xi) &= P_{j,2m+1}(\xi) + e^{i2\pi 2^j\xi}Q_{j,2m+1}(\xi),\\
P_{j+1,4m+3}(\xi) &= -P_{j,2m+1}(\xi) + e^{i2\pi 2^j\xi}Q_{j,2m+1}(\xi),\\
Q_{j+1,4m}(\xi) &= P_{j,2m}(\xi) \phantom{+P_{j,2m+1}(\xi)} - e^{i2\pi 2^j\xi}Q_{j,2m}(\xi),\\
Q_{j+1,4m+1}(\xi) &= P_{j,2m}(\xi) \phantom{+P_{j,2m+1}(\xi)} + e^{i2\pi 2^j\xi}Q_{j,2m}(\xi),\\
Q_{j+1,4m+2}(\xi) &= -P_{j,2m+1}(\xi) + e^{i2\pi 2^j\xi}Q_{j,2m+1}(\xi),\\
Q_{j+1,4m+3}(\xi) &= P_{j,2m+1}(\xi) + e^{i2\pi 2^j\xi}Q_{j,2m+1}(\xi),
\end{aligned} \tag{11}$$

with

$$\begin{aligned}
P_{1,0} = Q_{1,1} &= 1 + e^{i2\pi\xi}\ ,\\
P_{1,1} = Q_{1,0} &= 1 - e^{i2\pi\xi}\ ,
\end{aligned}$$

and for $j \geq 1$ and $m = 0, \ldots, 2^{j-1} - 1$. Note that P and Q in (11) are equal to the previous definition in (2) and (3) except for some changes of signs.

This section is dedicated to a rigorous proof of the symmetry (and the other desirable properties of the symmetric RST). The proof is 'constructive' in that it provides a simple way of applying the transform, namely by means of the Haar wavelet packet transform scheme.

The equations (11) can be written more compactly as

$$P_{j+1,m}(\xi) = (-1)^{m_1 m_2} P_{j,\lfloor m/2 \rfloor}(\xi) + (-1)^{m_1(m_2+1)} e^{i2\pi 2^j \xi} Q_{j,\lfloor m/2 \rfloor}(\xi), \tag{12}$$

$$Q_{j+1,m}(\xi) = (-1)^{(m_1+1)m_2} P_{j,\lfloor m/2 \rfloor}(\xi) + (-1)^{(m_1+1)(m_2+1)} e^{i2\pi 2^j \xi} Q_{j,\lfloor m/2 \rfloor}(\xi), \tag{13}$$

where m_1 and m_2 are the two least significant digits of the binary representation of m, and $\lfloor m/2 \rfloor$ means the biggest integer less or equal to $m/2$. Rewriting to the obvious matrix form yields

$$\begin{bmatrix} P_{j+1,m}(\xi) \\ Q_{j+1,m}(\xi) \end{bmatrix} = \begin{bmatrix} (-1)^{m_1 m_2} & (-1)^{m_1(m_2+1)} \\ (-1)^{(m_1+1)m_2} & (-1)^{(m_1+1)(m_2+1)} \end{bmatrix} \begin{bmatrix} P_{j,\lfloor m/2 \rfloor}(\xi) \\ e^{i2\pi 2^j \xi} Q_{j,\lfloor m/2 \rfloor}(\xi) \end{bmatrix}. \tag{14}$$

This latter form of the RS equations shows the core of the transform; the 2×2 matrix. Incidentally, this is also the 'secret' of the easy implementation.

To have a solid basis for the derivation of the RST properties, the first thing to do is to define exactly what the RST is.

Definition 9 (Symmetric Rudin-Shapiro Transform) *Define the mapping* $\mathbf{P}_{j,m} : \mathbb{R}^{2^j} \mapsto \mathbb{R}^{2^j}$, $j \geq 1$, *as*

$$\begin{bmatrix} y_k \\ y_{k+2^{j-1}} \end{bmatrix} = \frac{(-1)^{mk}}{\sqrt{2}} \begin{bmatrix} 1 & (-1)^k \\ (-1)^m & -(-1)^{k+m} \end{bmatrix} \begin{bmatrix} x_{2k} \\ x_{2k+1} \end{bmatrix} \tag{15}$$

for $k = 0, \ldots, 2^{j-1} - 1$ *when mapping* $\mathbf{x}$ *to* $\mathbf{y}$. *Define*

$$\mathbf{P}_j^{(J)} \equiv \begin{bmatrix} \mathbf{P}_{j,0} & & 0 \\ & \ddots & \\ 0 & & \mathbf{P}_{j,2^{J-j}-1} \end{bmatrix}, \tag{16}$$

and finally defined the Rudin-Shapiro transform $\mathbf{P}^{(J)}$ *and the auxiliary transform* $\mathbf{Q}^{(J)}$ *as*

$$\mathbf{P}^{(J)} \equiv \prod_{j=1}^{J} \mathbf{P}_j^{(J)}, \qquad \textit{and} \qquad \mathbf{Q}^{(J)} \equiv \prod_{j=1}^{J-1} \mathbf{P}_j^{(J)} \mathbf{P}_{J,1}. \tag{17}$$

Note that (15) is the inverse of the transform proposed in (14). The 2×2 matrix in (15) aside, it is not immediately obvious neither how this definition is linked to (11), nor that it defines a symmetric transform. However, the following theorem establishes that this definition does indeed provide the desired transform.

Theorem 10 (Properties of the Rudin-Shapiro Transform) *The Rudin-Shapiro transform* $\mathbf{P}^{(J)} : \mathbb{R}^{2^J} \mapsto \mathbb{R}^{2^J}$ *and the corresponding polynomials*

$$P_m^{(J)}(\xi) = \sum_{n=0}^{2^J-1} p_{m,n}^{(J)} e^{i2\pi n\xi}.$$

has the following properties:

(I) The rows of $\mathbf{P}^{(J)}$ *are the coefficients of the polynomials defined in* (11).

(II) The entries of $\mathbf{P}^{(J)} = \left[p_{m,n}^{(J)}\right]$ *are given by*

$$p_{m,n}^{(J)} = 2^{-J/2} \prod_{j=1}^{J} (-1)^{(m_j+n_{J-j+2})(m_{j+1}+n_{J-j+1})}, \tag{18}$$

for $m, n = 0, \ldots, 2^J - 1$*, where* m_j *are the* j*'th digit in the binary representation of* m*, with* m_1 *LSB.*

(III) It is an orthogonal and symmetric Hadamard matrix.

(IV) The non-zero even shifts of the auto correlation of $\mathbf{p}_m^{(J)}$ *equal zero, that is,*

$$\left(\mathbf{p}_m^{(J)} * \overline{\mathbf{p}_m^{(J)}}\right)[2k] = \delta[k]$$

for $k = -2^J + 1, \ldots, 2^J - 1$*.*

(V) It satisfies [2]

$$0 < |P_m^{(J)}(\xi)| < \sqrt{2}, \quad m = 0, \ldots, 2^J - 1, \tag{19}$$

on $(0; 1/2)$*. Moreover,*

$$P_{2j}(0) = P_{2j}(1/2) = 1, \tag{20}$$

and

$$P_{2j+1}(0) = \sqrt{2}, \quad P_{2j+1}(1/2) = 0, \tag{21}$$

and finally

$$P_j(1/4) = 1\ . \tag{22}$$

Proof To prove (I) first note

$$\mathbf{P}^{(j)} = \left(\mathbf{P}_{j,0}\right)^\top \begin{bmatrix} \mathbf{P}^{(j-1)} & \\ & \mathbf{Q}^{(j-1)} \end{bmatrix}, \tag{23}$$

$$\mathbf{Q}^{(j)} = \left(\mathbf{P}_{j,1}\right)^\top \begin{bmatrix} \mathbf{P}^{(j-1)} & \\ & \mathbf{Q}^{(j-1)} \end{bmatrix}.$$

[2] Only semi-flatness, and not near-flatness of the polynomials is actual proven here. However, the author feels sufficiently confident about the validity of the statement to include it in the theorem.

This follows from

$$\begin{aligned}
&\left(\mathbf{P}_{j,0}\right)^\top \begin{bmatrix} \mathbf{P}^{(j-1)} & \\ & \mathbf{Q}^{(j-1)} \end{bmatrix} \\
&\qquad = \left(\mathbf{P}_{j,0}\right)^\top \begin{bmatrix} \mathbf{P}_{j-1,0} & \\ & \mathbf{P}_{j-1,1} \end{bmatrix}^\top \begin{bmatrix} \mathbf{P}^{(j-2)} & & & \\ & \mathbf{Q}^{(j-2)} & & \\ & & \mathbf{P}^{(J-2)} & \\ & & & \mathbf{Q}^{(j-2)} \end{bmatrix} \\
&\qquad \vdots \\
&\qquad = \prod_{k=j}^{1} \left(\mathbf{P}_k^{(j)}\right)^\top \\
&\qquad = \mathbf{P}^{(j)}.
\end{aligned}$$

Note also that $\left(\mathbf{P}_{j,0}\right)^\top$ is the transform given as

$$\begin{bmatrix} x_{2k} \\ x_{2k+1} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ (-1)^k & -(-1)^k \end{bmatrix} \begin{bmatrix} y_k \\ y_{k+2^{j-1}} \end{bmatrix}$$

for $k = 0, \ldots, 2^{j-1} - 1$ when mapping $\mathbf{y}$ to $\mathbf{x}$. So

$$\left(\mathbf{P}_{j,0}\right)^\top = \frac{1}{\sqrt{2}} \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix} & & \begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} & \\ & \ddots & & \ddots \\ & & \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix} & & \begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \end{bmatrix}_{2^j \times 2^j}$$

Letting $\mathbf{p}_m^{(j)}$ denote the m'th row of $\mathbf{P}^{(j)}$, and likewise with $\mathbf{Q}^{(j)}$, it follows that

$$\mathbf{P}^{(j)} = \Big(\mathbf{P}_{j,0}\Big)^\top \begin{bmatrix} \mathbf{P}^{(j-1)} & \\ & \mathbf{Q}^{(j-1)} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{p}_0^{(j-1)} & \mathbf{q}_0^{(j-1)} \\ \mathbf{p}_0^{(j-1)} & -\mathbf{q}_0^{(j-1)} \\ \mathbf{p}_1^{(j-1)} & \mathbf{q}_1^{(j-1)} \\ -\mathbf{p}_1^{(j-1)} & \mathbf{q}_1^{(j-1)} \\ \vdots & \vdots \\ \mathbf{p}_{2^j-2}^{(j-1)} & \mathbf{q}_{2^j-2}^{(j-1)} \\ \mathbf{p}_{2^j-2}^{(j-1)} & -\mathbf{q}_{2^j-2}^{(j-1)} \\ \mathbf{p}_{2^j-1}^{(j-1)} & \mathbf{q}_{2^j-1}^{(j-1)} \\ -\mathbf{p}_{2^J-1}^{(j-1)} & \mathbf{q}_{2^j-1}^{(j-1)} \end{bmatrix}, \tag{24}$$

which demonstrates the appending rule defined in the first four equations of (11). A similar calculation will show the last four equations.

The proof of (II) goes by induction on (18). In the following the scaling $2^{-J/2}$ is ignored. For $J = 1$

$$\mathbf{P}^{(1)} = \begin{bmatrix} p_{0,0}^{(1)} & p_{0,1}^{(1)} \\ p_{1,0}^{(1)} & p_{1,1}^{(1)} \end{bmatrix} = \begin{bmatrix} (-1)^{(0+0)(0+0)} & (-1)^{(0+0)(0+1)} \\ (-1)^{(1+0)(0+0)} & (-1)^{(1+0)(0+1)} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

which is correct according to (15). Assume that (18) is true for j. From (24) it follows that

$$p_{m,n}^{(j+1)} = \begin{cases} (-1)^{m_2 m_1} p_{\lfloor m/2 \rfloor, n}^{(j)} & \text{for } 0 \le n < 2^j \\ (-1)^{(m_2+1)m_1} q_{\lfloor m/2 \rfloor, n-2^j}^{(j)} & \text{for } 2^j \le n < 2^{j+1}. \end{cases} \tag{25}$$

The first case can be rewritten

$$\begin{aligned} (-1)^{m_2 m_1} p_{\lfloor m/2 \rfloor, n}^{(j)} &= (-1)^{m_2 m_1} \prod_{k=1}^{j} (-1)^{(m_{k+1}+n_{j-k+2})(m_{k+2}+n_{j-k+1})} \\ &= (-1)^{(m_1+n_{j+2})(m_2+n_{j+1})} \prod_{k=2}^{j+1} (-1)^{(m_k+n_{j+1-k+2})(m_{k+1}+n_{j+1-k+1})} \\ &= \prod_{k=1}^{j+1} (-1)^{(m_k+n_{j+1-k+2})(m_{k+1}+n_{j+1-k+1})} \end{aligned}$$

for $n = 0, \ldots 2^j - 1$. To rewrite the second case, the connection between $p_{m,n}^{(j)}$ and

$q^{(j)}_{m,n}$ are derived. From (11) it is seen that

$$\begin{aligned} Q_{j+1,4k}(\xi) &= P_{j+1,4k+1}(\xi)\ , \\ Q_{j+1,4k+1}(\xi) &= P_{j+1,4k}(\xi)\ , \\ Q_{j+1,4k+2}(\xi) &= P_{j+1,4k+3}(\xi)\ , \\ Q_{j+1,4k+3}(\xi) &= P_{j+1,4k+2}(\xi)\ . \end{aligned} \tag{26}$$

Changing the sign in this manner can be accomplished by adding 1 to the LSB of the row counter variable, that is to m_1. Thus,

$$q^{(j)}_{m,n} = (-1)^{(m_1+1)(m_2+n_j)} \prod_{k=2}^{j} (-1)^{(m_k+n_{j-k+2})(m_{k+1}+n_{j-k+1})}\ ,$$

and the second case of (25) can now be rewritten

$$\begin{aligned} (-1)^{(m_2+1)m_1} q^{(j)}_{\lfloor m/2\rfloor, n-2^j} &= (-1)^{(m_2+1)m_1}(-1)^{(m_2+1)(m_3+n_j)} \\ &\qquad \times \prod_{k=2}^{j} (-1)^{(m_{k+1}+n_{j-k+2})(m_{k+2}+n_{j-k+1})} \\ &= (-1)^{(m_1+n_{j+2})(m_2+n_{j+1})}(-1)^{(m_2+n_{j+1})(m_3+n_j)} \\ &\qquad \times \prod_{k=3}^{j+1} (-1)^{(m_k+n_{j+1-k+2})(m_{k+1}+n_{j+1-k+1})} \\ &= \prod_{k=1}^{j+1} (-1)^{(m_k+n_{j+1-k+2})(m_{k+1}+n_{j+1-k+1})} \end{aligned}$$

for $n = 2^j, \ldots 2^{j+1}-1$. The second last equality is due to $n_{j+1} = 1$ and $n_{j+2} = 0$. This proves (18).

The orthogonality of $\mathbf{P}^{(J)}$ stated in (III) follows immediately from orthogonality of $\mathbf{P}_{j,m}$, and according to (II) $\mathbf{P}^{(J)}$ is a Hadamard matrix. The symmetry can be established by interchanging m and n in the power of (-1) in (18) and substituting $k = J - j + 1$. This yields

$$\begin{aligned} p^{(J)}_{n,m} &= 2^{-J/2} \prod_{j=1}^{J} (-1)^{(n_j+m_{J-j+2})(n_{j+1}+m_{J-j+1})} \\ &= 2^{-J/2} \prod_{k=J}^{1} (-1)^{(n_{J-k+1}+m_{k+1})(n_{J-k+2}+m_k)} \\ &= p^{(J)}_{m,n} \end{aligned}$$

demonstrating that interchanging m and n in (18) is equivalent to reversing the order of multiplication. It follows that the matrix $\mathbf{P}^{(N)}$ is symmetric.

The property (IV) follows from Lemma 7 which apply unchanged to the symmetric case (the calculations in the proof of the lemma are independent of the position of the one minus in the definitions of $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$).

The near-flat polynomial property in (V) has already been demonstrated as far as semi-flatness. However, despite a significant effort any attempt by the author to find a proof of near-flatness of the polynomials on $(0; 1/2)$ have been fruitless.

The equations (20) and (21) follows from a series of calculations equivalent to those in the proof of Lemma 5. A rewriting of (12) in the same fashion as (9) yields

$$\left.\begin{matrix} P_{j+2,m}(\xi) \\ Q_{j+2,m}(\xi) \end{matrix}\right\} = \left(\pm 1 \pm e^{i2\pi 2^{j+1}\xi}\right) P_{j,u}(\xi) + e^{i2\pi 2^{j}\xi}\left(\pm 1 \pm e^{i2\pi 2^{j+1}\xi}\right) Q_{j,u}(\xi)$$

where the two signs inside each of the parentheses will be the same in the one and opposite in the other parenthesis, e.g. $++$ and $+-$. Thus,

$$\begin{aligned} \left.\begin{matrix} P_{j+2,m}(1/4) \\ Q_{j+2,m}(1/4) \end{matrix}\right\} &= \left(\pm 1 \pm e^{i2\pi 2^{j-1}}\right) P_{j,u}(1/4) + e^{i2\pi 2^{j-2}}\left(\pm 1 \pm e^{i2\pi 2^{j-1}}\right) Q_{j,u}(1/4) \\ &= \begin{cases} \pm 2P_{j,u}(1/4) & \text{for some } m \\ \pm 2Q_{j,u}(1/4) & \text{for the other } m\ . \end{cases} \end{aligned}$$

Then

$$|P_{2n,m}(1/4)| = |Q_{2n,m}(1/4)| = 2^{n-1}|P_{2,u}| = 2^{n-1}|Q_{2,u}| = 2^n$$

and

$$|P_{2n-1,m}(1/4)| = |Q_{2n-1,m}(1/4)| = 2^{n-1}|P_{1,u}| = 2^{n-1}|Q_{1,u}| = \sqrt{2}\cdot 2^{n-1}\ .$$

This proves (22). □

The theorem established a close connection between the properties of the Rudin-Shapiro polynomials and the transform. In particular, the spread spectrum property which is an intrinsic attribute of the polynomials, is inherited by the transform. The particular 'distribution' of signs in the construction makes the transform symmetric, and thus its own inverse.

4.2 Fast Implementation

The definition of the RST given in Definition 9 is based on the recursive construction process of RS polynomials. When writing this process in matrix form the 2×2 matrix in (15) emerges along with the $2^J \times 2^J$ matrix in (16). The combination of these two matrices is the key to a fast implementation.

The matrices $\mathbf{P}_j^{(J)}$ provide a factorization of the RST matrix, and the 2×2 matrix gives a simple and easy $O(N)$ implementation of each of the $\mathbf{P}_j^{(J)}$ matrices. The

principle is here demonstrated with a size 8×8 transform, but easily applies to all size 2^J RSTs. The first factor to be applied in the 8×8 case is $\mathbf{P}_3^{(3)} = \mathbf{P}_{3,0}$. That is,

$$\mathbf{P}_3^{(3)} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

This is equivalent to a Haar wavelet transform except the filter taps are changing during filtering. The result of transforming with this matrix can be considered as two parts of length 4. In the Haar case the two parts can be identified as a low and high pass part, respectively, while in the RST case the constant change of filter taps results in two parts containing a mix of frequencies. The splitting into two signal parts is also illustrated in Fig. 3 by the first (top) set of arrows. The next step in the transform is

$$\mathbf{P}_2^{(3)} = \begin{bmatrix} \mathbf{P}_{2,0} & \\ & \mathbf{P}_{2,1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & & & & \\ 0 & 0 & 1 & -1 & & & & \\ 1 & -1 & 0 & 0 & & & & \\ 0 & 0 & 1 & 1 & & & & \\ & & & & 1 & 1 & 0 & 0 \\ & & & & 0 & 0 & -1 & 1 \\ & & & & -1 & 1 & 0 & 0 \\ & & & & 0 & 0 & 1 & 1 \end{bmatrix},$$

i.e. the same procedure is repeated (independently) on each of the two signal parts. Notice that $m = 0$ when transforming the first part and $m = 1$ when transforming the second part of the signal. The m makes the transform symmetric in the sense that $m = 0$ throughout the transform steps would produce the non-symmetric RST. This second step is shown as the second set of eight arrows (from the top) in Fig. 3.

The final step is

$$\mathbf{P}_1^{(3)} = \begin{bmatrix} \mathbf{P}_{1,0} & & & \\ & \mathbf{P}_{1,1} & & \\ & & \mathbf{P}_{1,2} & \\ & & & \mathbf{P}_{1,3} \end{bmatrix} = \begin{bmatrix} 1 & 1 & & & & & & \\ 1 & -1 & & & & & & \\ & & 1 & 1 & & & & \\ & & -1 & 1 & & & & \\ & & & & 1 & 1 & & \\ & & & & 1 & -1 & & \\ & & & & & & 1 & 1 \\ & & & & & & -1 & 1 \end{bmatrix}.$$

As a result of the factorization the RST can be applied in J steps by multiplying a signal with all of the $\mathbf{P}_j^{(J)}$ matrices (in the right order). Each multiplication is an $O(N^2)$ operation, but the mapping given in (15) shows how to reduce the multiplication to an $O(N)$ filtering process. For any choice of m and k the 2×2 matrix contains three times $+1$ and one -1. Consequently, the output of the mapping is merely a sequence of sums and differences of sample pairs. A division by $\sqrt{2}$ should be applied to every sum/difference, but since the mapping is linear this scaling can be applied as division by 2 for every other step in the transform. Note that division by 2 is equivalent to a binary shift of 1.

When implementing the RST according to this scheme it is obviously important to get the 2×2 matrix correct. The m and k change constantly as the transform is applied. In Fig. 3 these changes are shown along with the 2×2 matrix for each sample pair in each step of the transform.

Applying a linear transform to a signal is basically a set of inner products with the row vectors of the transform matrix. In the case of the RST these vectors are ± 1's only, and consequently the RST is numerically very stable as all signal samples are weighted equally. This property is preserved in the fast implementation where each transform step also consists of ± 1's only. The fact that each intermediate sample depends on only two other samples makes the fast implementation even more stable than the matrix multiplication implementation. The normalization by 2 in every other transform step possess only negligible problems in the vast majority of applications.

The actual implementation of the RST can be accomplished by a regular filtering process divided into four steps, for even and odd k and m, which are used in the order needed, as demonstrated in Fig. 3. By doing this it is possible to avoid the computational demanding powers of (-1) in (15). For more details, see [24].

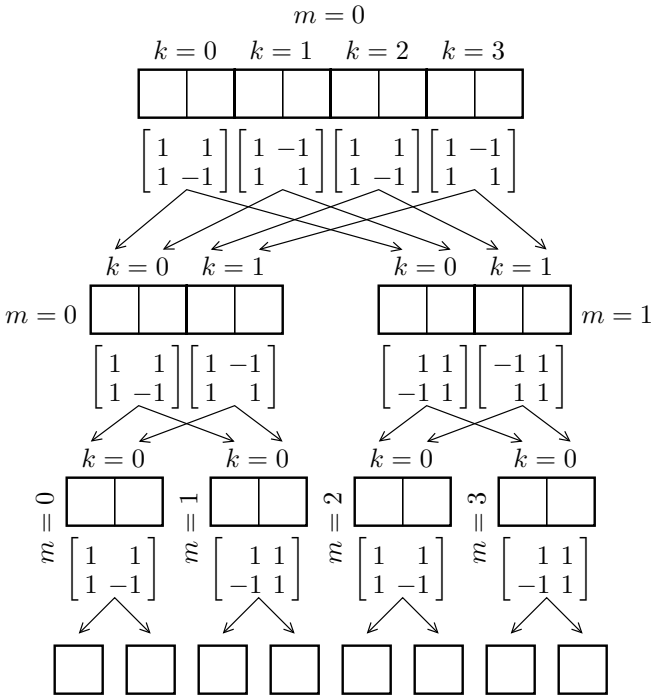

Fig. 3. This figure shows how the value of the variables change in the fast implementation of a symmetric RST. Here applied to a vector in $\mathbb{R}^8$.

4.3 Relation to the Haar Wavelet Packet Transform

Suppose that the same 2×2 matrix is used in all transform steps, i.e. suppose that m and k equal zero in all cases. The result is then a full decomposition wavelet packet Haar transform. The Haar transform is also its own inverse. If only m (but not k) is fixed at zero the result is the non-symmetric RST presented in (10). This is easily seen as

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\epsilon_n} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & (-1)^{\epsilon_n} \\ 1 & -(-1)^{\epsilon_n} \end{bmatrix}.$$

The relation to the Haar transform can also provide an explanation for the spread spectrum property without involving the RS polynomials. The Haar transform is a decomposition into a frequency localizing basis since the Haar filters are low and high pass filters (with two filter taps). This means that each element in the output from the (full decomposition) Haar transform represents the energy in a certain frequency range of the original signal. The RST does in some sense the exact opposite of this. Instead of applying the same filter to all samples pairs (and thereby creating a output localized in frequency) the RST applies the low and high pass filters alternately to sample pairs. The result is an output where the samples are the same as in the Haar transform case, but where the low and high pass samples are interleaved such that there is virtually no frequency localization in the resulting signal.

The close relation to the Haar wavelet packet transform provides another interesting property; instead of doing all the steps in the RST one can choose do only some of the steps and thereby obtain a different decomposition of the transformed signal. This is equivalent to selecting a particular basis in the Haar wavelet packet decomposition for representing the signal. Consequently, some of the theory regarding wavelet bases for $\mathbb{R}^N$ applies. For instance, the RST can be used to generate a number of spread spectrum signals which is equal to the number of different possible representations in the wavelet packet decomposition. A lower bound for this number is $2^{2^{J-1}}$, see Jensen and la Cour-Harbo [20]. And the best basis search algorithm can be applied to find the best, in some defined sense, sequence.

4.4 Other Properties of RS Polynomials

The work with RS polynomials and sequences have led the author to believe in some other properties for which no proofs have yet been devised. These results are presented here as conjectures, and without any further explanations. So far, these results have found no practical use.

The first conjecture states that although the individual RS polynomials are (supposedly) near-flat on $(0; 1/2)$ they are not flat on $(0; 1/2)$.

Conjecture 1 *Let $P_{j,m}(\xi)$ be one of the polynomials defined in* (11)*. Then*

$$\lim_{j\to\infty} 2^{-j/2} \max_{\xi\in(0;1/2)} |P_{j,m}(\xi)| = \sqrt{2}$$

and the convergence is of order $O(e^{-j})$.

It seems that polynomials are equal in equidistant points with a finer resolution for longer polynomials

Conjecture 2 *Let $P_{j,k}(\xi)$ be one of the polynomials defined in* (11)*. Then*

$$2|P_{j,k}\Big(m2^{-j}\Big)| = |P_{j+2,k}\Big(m2^{-j}\Big)|, \quad k, m = 0, \ldots, 2^j - 1 \; .$$

In the limit this 'result' becomes

Conjecture 3 *The limits*

$$\lim_{j\to\infty} 2^{-j} P_{2j,k}(\xi) \qquad \textit{and} \qquad \lim_{j\to\infty} 2^{-j} P_{2j+1,k}(\xi)$$

converge pointwise on the dense subset $\Big\{m2^{-n}; m = 0, \ldots, 2^n\Big\}_{n\in\mathbb{N}}$ of the unit interval.

The recursive construction of the polynomials means that there are many different relations between the various polynomials. A few has been conjectured upon here, and others can easily be discovered by experiments.

5 Acknowledgement

The author would like to thank Lars Villemoes for his useful suggestions and discussions in the field of spread spectrum sequences. The author would also like to thank Harold Shapiro for interesting discussions and for providing a copy of his 1951 Master's thesis [36].

References

[1] J.-P. Allouche and M.M. France. On an extremal property of the Rudin-Shapiro sequence. *Mathematika*, 32:33–38, 1985.

[2] J. Beck. Flat polynomials on the unit circle. *Bull. London Math. Soc.*, 23:269–277, 1991.

[3] E. Beller. Polynomial extremal problems in L^p. *Proc. Amer. Math. Soc*, 30(2):249–259, 1971.

[4] G. Benke. Generalized Rudin-Shapiro systems. *J. Fourier Anal. Appl.*, 1(1):87–101, 1994.

[5] J. Brillhart. On the Rudin-Shapiro polynomials. *Duke Math. J.*, 40:335–353, 1973.

[6] John Brillhart and Patrick Morton. Über Summen von Rudin-Shapiroschen Koeffizienten. *Illinois J. Math.*, 22(1):126–148, 1978.

[7] J. S. Byrnes. On polynomials with coefficients of modulus one. *Bull. London Math. Soc.*, 9:171–176, 1977.

[8] J. S. Byrnes. Quadrature Mirror Filters, Low Crest Factor Arrays, Functions Achieving Optimal Uncertainty Principle Bounds, and Complete Orthonormal Sequences – A Unified Approach. *App. and Comp. Harm. Anal.*, 1:261–266, 1994.

[9] J. S. Byrnes. *Signal and Image Representations in Combined Spaces*, volume 7 of *Wavelet analysis and its applications*, chapter A Low Complexity Energy Spreading Transform Coder, pages 167–187. Academic Press, 1998.

[10] J. S. Byrnes, I. Gertner, G. Ostheimer, and M.A. Ramalho. Discrete one dimensional signal processing apparatus and method using energy spreading coding, June 15, 1999. U.S. Patent no. 5,913,186.

[11] J. S. Byrnes, B. Saffari, and H.S. Shapiro. Energy Spreading and Data Compression Using the Prometheus Orthonormal Set. In J.M. Lervik and P. Waldemar, editors, *Digital Signal Processing Workshop Proceedings*, pages 0–12. IEEE, September 1996.

[12] J.C. Clunie. The minimum modulus of a polynomial on the unit circle. *Quart. Jour. Math.*, 10(2):95–98, 1959. Oxford.

[13] R. Coifman, F. Geshwind, and Y. Meyer. Noiselets. *App. and Comp. Harm. Anal.*, 10:27–44, 2001. Was available as preprint in 1994.

[14] P. Erdös. Some unsolved problems. *Michigan Math. J.*, 4:291–300, 1957.

[15] M. L. Fredman, B. Saffari, and B. Smith. Polynômes réciproques: conjecture d'Erdös en norme L^4, taille des autocorrélations et inexistence des codes de Barker. *C. R. Acad. Sci. Paris Sér. I Math.*, 308(15):461–464, 1989.

[16] M. J. E. Golay. Multislit spectrometry. *J. Optical Soc. Amer.*, 39:437–444, 1949.

[17] M. J .E. Golay. Static multislit spectroscopy and its applications to the panoramic display of infrared spectra. *J. Opt. Soc. Amer.*, 41:468 – 472, 1951.

[18] M. J. E. Golay. Complementary series. *IRE Trans.*, IT-7:82–87, 1961.

[19] G. H. Hardy and J. E. Littlewood. Some problems of Diophantine approximation: A remarkable trigonometrical series. *Proc. National Acad. Sc.*, 2:583–586, 1916.

[20] A. Jensen and A. la Cour-Harbo. *Ripples in Mathematics - The Discrete Wavelet Transform*. Springer, Heidelberg Berlin, june 2001.

[21] J.-P. Kahane. Sur les polynomes a coefficients unimodulaires. *Bull. London Math. Soc.*, 12:321–342, 1980.

[22] T.W. Körner. On a polynomial of Byrnes. *Bull. London Math. Soc.*, 12:219–224, 1980.

[23] A. la Cour-Harbo. *Robust and Low-Cost Active Sensors by means of Signal Processing Algorithms*. PhD thesis, Aalborg University, August 2002.

[24] A. la Cour-Harbo. The symmetric rudin-shapiro transform - an easy, stable, and fast construction of multiple orthogonal spread spectrum signals. In *IEEE Proceedings of Acou., Speech, and Sig. Proc.*, volume 6, pages 397 – 400, 2003.

[25] J.E. Littlewood. On the mean values of certain trigonometric polynomials (ii). *Illinois J. of Math*, 6:1 – 39, 1962.

[26] J.E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$. *J. London Math. Soc.*, 41:367–376, 1966.

[27] M. Mendès France and G. Tenenbaum. Dimension des courbes planes, papiers pliés et suites de Rudin-Shapiro. *Bull. Soc. Math. France*, 109(2):207–215, 1981.

[28] M. Nazarahty, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, and W.R. Trutna Jr. Real-time long range complementary correlation optical time domain reflectometer. *IEEE J. Lightwave Tech.*, 7:24 – 38, 1989.

[29] D.J. Newman. An l^1 extremal problem for polynomials. *Proc. Amer. Math. Soc.*, 16:1287 – 1290, 1965.

[30] J.-S. No, H. Chung, and M.-S. Yun. Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$. *IEEE Trans. Inform. Theory*, 44(3):1278 – 1282, May 1998.

[31] J.-S. No, S.W. Golomb, G. Gong, H.-K. Lee, and P. Gaal. Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. *IEEE Trans. Inform. Theory*, 44(2):814 –817, March 1998.

[32] J.-S. No and P.V. Kumar. A new family of binary pseudorandom sequences having optimal periodic correlation properties and larger linear span. *IEEE Trans. Inform. Theory*, 35(2):371 – 379, March 1989.

[33] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.

[34] Bahman Saffari. Une fonction extrémale liée à la suite de Rudin-Shapiro. *C. R. Acad. Sci. Paris Sér. I Math.*, 303(4):97–100, 1986.

[35] Bahman Saffari and Brent Smith. Sur une note récente relative aux polynômes à coefficients ± 1 et à la conjecture d'Erdös. *C. R. Acad. Sci. Paris Sér. I Math.*, 310(7):541–544, 1990.

[36] H. S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, Massachusetts Institute of Technology, may 1951.

[37] M. Taghavi. An estimate on the correlation coefficients of the Rudin-Shapiro polynomials. *Iranian J. Sci. Tech.*, 20(2, Trans. A Sci.):235–240, 1996.

[38] M. Taghavi. Upper bounds for the autocorrelation coefficients of the Rudin-Shapiro polynomials. *Korean J. Comput. Appl. Math.*, 4(1):39–46, 1997.

[39] C.-C. Tseng. Signal multiplexing in surface-wave delay lines using orthogonal pairs of golay's complementary sequences. *IEEE Trans. Sonics Ultrason.*, SU-18:103 – 107, 1971.

[40] A. Zygmund. *Trigonometrical series*. Warsaw, 1935.